OIPE JC162
APR 0 5 2001
PATENT & TRADEMARK OFFICE

09728727 .040501

Holiday e-mails can carry a danger

Experts are warning about viruses in infected attachments

BY DAVID L. WILSON
Mercury News Washington Bureau

WASHINGTON — The holiday season is often a time when computer users pass around amusing electronic animations via e-mail. Although most of these attachments are harmless, some may hide destructive computer viruses.

Indeed, anti-virus watchdogs identified a new virus this week that masquerades as an innocuous bunch of digital photos but actually plants a time bomb that will erase the computer's hard drive on Jan. 1, 2000.

Because that's the same date that the Y2K bug is expected to cause many computer systems to crash, the virus might fool users into believing they have a Y2K problem.

Virus fighters expect more viruses linked to Y2K to emerge as Jan. 1 approaches, and they are once again begging computer users to avoid opening e-mailed attachments.

Virus fighters expect more viruses linked to Y2K to emerge as Jan. 1 approaches.

"We're telling people to be very wary of electronic Christmas cards," said Sal Viveros, a virus expert with Network Associates Inc., based in Santa Clara.

The Mypics worm, as this latest threat is called, arrives attached to what appears to be e-mail from a friend or associate that says, "Here's some pictures for you!"

Opening the attached file, Pics4You.exe, will infect your computer with the virus, which will at-

See *VIRUSES*, Page 3C

Fig. 1, page 1 of 2

OIPE JC182
APR 0 5 2001
& TRADEMARK OFFICE

Holiday e-mails carry risk

VIRUSES

from Page 1C

tempt to mail itself to 50 people it finds in your Microsoft Outlook e-mail address book. It will also change the home page of your Microsoft Internet Explorer Web browser to a pornographic site.

The real damage occurs Jan. 1, when the virus will change the computer's most basic software and attempt to erase the hard drive.

The increasing frequency of alerts relating to things like electronic viruses is prompting renewed calls for safe computing, but few experts expect users to change their habits.

"It would be great if everybody followed the rule: Never open e-mail attachments if you can help it," said Carey Nachenberg, chief researcher at Symantec's anti-viral research center. "But I don't think they will."

In general, just looking at an infected e-mail can't hurt; users have to do something else to activate the virus and infect their system. Typically, a virus comes as an attachment to e-mail, such as a document that can be read only with a word processor like Microsoft Word.

Clicking on the attachment to read the document can infect the user's machine with any virus that was lurking on the sender's machine. A virus is dangerous because it can alter or destroy data.

Until recently, experts advised users to simply avoid opening attachments sent by people they didn't know. Unfortunately, the most troublesome viruses today spread by fooling people into believing the document was sent by a friend.

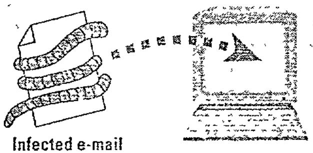
For instance, Mypics attempts to mail copies of itself to anyone in the user's e-mail address book. Anyone receiving such a missive from, say, their brother, might open that attachment without thinking about it.

Most software vendors are aware of the problem and take steps to get around it. For instance, Blue Mountain Arts, a purveyor of electronic greeting cards, doesn't send the card via e-mail, just a Web address, which can be accessed though any browser.

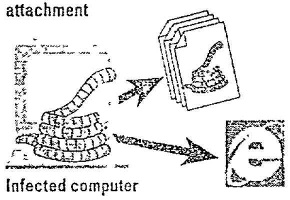
Jared P. Schutz, the company's executive director, said that's the only way to be safe. "I would highly recommend that people avoid opening attached files, even from people that they know," he said.

A computer virus for Christmas

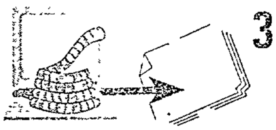
Many computer viruses travel as innocent-looking files attached to electronic mail. With the holiday season upon us, people often e-mail electronic greetings and photographs to friends and family members, but not every file that comes with an e-mail is safe. This year poses special hazards, according to anti-virus experts, because many virus writers may use the Y2K bug to hide their mischief. This week, anti-virus companies detected a new virus, named Mypics, that could erase a computer's hard drive on Jan. 1.



1 WORM ARRIVES
You get an e-mail with an attachment named Pics4You.exe saying, *"Here's some pictures for you!"*



2 WORM REPRODUCES
If you open the attachment, the worm will send itself to 50 people in your Microsoft Outlook address book. It also changes the home page of your Microsoft Internet Explorer browser to a pornographic site.



3 WORM WAITS
On Jan. 1, 2000, the worm will overwrite key system data. The user will see an apparent Y2K-related error when starting up the computer. The worm will then destroy all data on the hard drive.

HOW TO PROTECT YOURSELF

Avoid opening attachments to e-mail if possible. If you want the attachment, call the sender and verify its contents before opening it. Update virus protection software weekly and use it to scan attachments. Back up critical data regularly.

Source: Symantec Corp

MERCURY NEWS

That's the standard advice, but nobody expects attachments to disappear tomorrow, despite the warnings.

"I can't tell you whether we've still got a lot of people who just haven't gotten the message — newbies — or whether it's people who should know better but do it anyway," said Sandra Sparks, director of the Energy Department's Computer Incident Advisory Capability, which works to ensure the security of government computer systems. "Maybe it's the same kind of thing that happens with people who don't wear a seat belt."

Although many corporations scan all incoming e-mail and destroy any known virus before it's delivered into an employee's mailbox, very few Internet service providers offer such a feature, largely because examining every single data packet that flows into the pipes can slow service.

So for now, anti-virus protection is largely the responsibility of individuals.

To protect against all viruses, experts say virus protection software should be updated weekly.

Attachments generally should be avoided. If you receive an attachment that you want, contact the sender and ask if it was deliberately sent. If possible, ask that the information in the attachment be copied and pasted into a plain e-mail file and resent, or posted on a Web page.

If that's not possible and you must open the attachment, make sure it's scanned first with an updated anti-viral program.

Even with such precautions, it's still possible for a new, fast-moving virus to get through your defenses. The only real protection users have is to regularly make copies of the data on their hard drive

"Back up your critical stuff at least once a week," said Sparks. "I know that's annoying, and I know it takes time. But compare that amount of time vs. the amount of time you'd spend trying to rebuild your system, or your company, and that's a very small investment."

Contact David Wilson at (202) 383-6020 or at dwilson@sjmercury.com.

Fig. 1, page 2 of 2